ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

Evaluasi Manajemen Risiko Teknologi Informasi Berdasarkan *Framework* COBIT 5 Pada PT.BTM

Rival Dwi Anggriyan Putra[1], Eman Setiawan [2], Awalludiyah Ambarwati [3]
[1,2,3] Program Studi Sistem Informasi , Fakultas Ilmu Komputer, Universitas Narotama Surabaya
email : [1]rivaldwi.anggriyan@fik.narotama.ac.id, [2]eman.setiawan@narotama.ac.id ,
[3]ambarwati1578@gmail.com

Abstrak

Teknologi Informasi (TI) merupakan faktor pendukung dalam meningkatkan proses bisnis dalam sebuah perusahaan jasa pengiriman, tak terkecuali pada PT.BTM merupakan suatu perusahaan yang bergerak dalam bidang jasa pengiriman, perusahaan ini telah memanfaatkan teknologi dan memiliki software. Penggunaan sistem informasi pastinya memiliki banyak sebuah permasalahan, jika terjadi masalah akan berdampak secara kesuluruhan perusahaan. Seperti permasalahan yang sering terjadi pada PT.BTM berupa salah penginputan data kiriman berakibat lambat update status pengiriman. Yang mungkin dapat terjadi seperti sistem layanan tidak jalan atau masalah lain yang dapat merugikan perusahaan bahkan dapat menghancurkan perusahaan. Maka penilitian ini perlu dilakukan agar mengetahui sebuah penilaian manajemen risiko. Untuk meminimalkan kerugian maka digunakan framework COBIT 5 untuk mengevaluasi manajemen risiko TI. Proses evaluas pada penelitian inii terdiri beberapa tahapan, antara lain pengumpulan data, analisis data, analisis risiko. Hasil dari penilitian adalah dokumen yang berisi penilaian risiko TI dan langkah mitigasi yang sesuai dengan proses pemetaan COBIT 5 for risk serta usulan rekomendasi dari kami.

Kata kunci: *Manajemen risiko, COBIT 5 for Risk, penilaian risiko*

Abstract

Information Technology (IT) is a supporting factor in improving business processes in shipping companies, and PTBTM is an exception for a company engaged in shipping services, this company has used technology and used software. The use of information systems certainly has many problems, if a problem occurs it will have an impact on the overall company. As is often the case with PT. BTM, it is wrong to input shipment data resulting in slow delivery status updates. That might happen like a service system that cannot be done by the company. So this research needs to be done so that it can be known. To lend losses, a COBIT 5 framework is used to compensate for the loss of IT management. The evaluation process in this study consists of several stages, including data collection, data analysis, risk analysis. The results of the research are documents that contain IT financial statements and mitigation measures that are in accordance with the COBIT 5 process for risk and our contribution assessment.
.

Keywords*: Risk management, COBIT 5 for Risk, Risk assessment*

1. Pendahuluan

PT.BTM perusahaan yang bergerak dalam bidang jasa pengiriman yang telah menggunakan dan memanfaatkan teknologi informasi dalam menjalankan proses bisnisnya. Permasalahan yang pernah terjadi pada perusahaan bymatrans ialah mengenai pencurian data pelanggan, serta sering terjadi permasalahan mengenai salah *input* data kiriman dan jarang-jarang PC mengalami *erorr* pada saat melakukan pelayanan.

Risiko merupakan kombinasi dari probabilitas suatu peristiwa sedangkan Manajemen risiko salah satu tujuan dari perusahaan dalam mengakui risiko, menilai

dampak dan kemungkinan risiko dan mengembangkan strategi, seperti menghindari risiko, mengurangi efek negatif dari risiko atau mentransfer risiko, untuk mengelolanya dalam konteks selera risiko perusahaan [1]. Pengertian lain dari tentang manajemen risiko teknologi informasi menurut *National Institute of Standards and Technology*, manajemen risiko meliputi tiga proses, yaitu *risk assesment, risk mitigation, evaluation assesment* [2].

1. ***Risk assesment*** adalah tahap suatu risiko diidentifikasi dan mencari dampak risiko untuk mencari kontrol mitigasi yang sesuai
2. ***Risk Mitigation*** adalah tahap memprioritaskan tingkat keparahan risiko lalu mengevaluasi penyebab dan dampak risiko dan impelementasikan kontrol yang tepat dalam mengurangi risiko yang sudah diketahui pada proses risk.
3. ***Evaluation and assessment*** adalah tahap ini merupakan kunci dari proses manajemen risiko dilakukan, dimana risiko yang telah di evaluasi ditindaklanjuti dengan diberikan panduan *best pratice* agar manajemen riisko yang dilakukan berhasil.

COBIT 5 *for Risk* memiliki perspektif manajemen risiko yang terkait cara melakukan proses identifikasi, analisis, dan cara untuk merespon risiko. Perspektif ini membutuhkan dua domain *risk processes* untuk diimpelementasikan, yaitu EDM03 *Ensure Risk Optimisation* dan AP012 *Manage risk* [3].

Aset TI merupakan komponen yang penting dalam suatu perusahaan tidak adanya aset TI dalam perusahaan pada zaman sekarang perusahaan akan susah dijalankan, membagi aset TI menjadi dua yaitu *IT Asset Tangible* dan *IT Asset Intangible. IT Asset Tangible* merupakan aset perusahaan yang secara nyata dapat langsung digunakan untuk keutungan pribadi atau keuntungan perusahaan seperti komputer, *hardware*, *database, server* sedangkan *IT Asset Intangible* merupakan aset perusahaan yang tidak nyata berupa *software application, security program* dan *license software* [4].

Dalam penelitian sebelumnya melakukan penilaian risiko untuk risiko DPTSI [5], berfokus pada penilaian risiko terhadap proses TI yang terdapat pada unit *helpdesk* Subdirektorat layanan teknologi dan Sistem Informasi DPTSI ITS Surabaya berdasarkan COBIT 5 *for risk,* Untuk standar risiko merujuk pada domain DSS02 *Manage Service Requests* and Incidents dan AP012 *Manage risk,* Disisi lain terdapat penelitian mengenai bagaimana mecapai keberhasilan impelementasi ERP berdasarkan ketentuan faktor keberhasilan kritis. Penilaian risiko dilakukan dengna menggunakan COBIT 5 untuk standar risiko dengan merujuk ke domain AP012 *manage risk,* dalam penelitiannya menggunakan dua standar, yaitu CSF dari impelementasi post ERP dan COBIT 5 untuk risiko. Namun, penelitian tersebut dilakukan tidak melakukan analisis risiko secara terperinci. Selain itu, juga tidak menggambarkan detail jenis risiko, skenario risiko. Cuma menggambarkan secara singkat cara penyelesaian penilaian risiko [6]. Untuk penelitian mengenai pengelolaan risiko aset TI, perhitungan nilai risikonya menggunakan metode fmea kuantitatif tetapi tidak menjelaskan cara distribusi mitigasi risikonya [7] .

Dengan demikian, perlu dilakukan sebuah penelitian mengenai penilaian manajemen risiko sehingga perusahaan dapat memperkecil risiko yang akan timbul. Tujuan penelitian ini mencegah agar tidak mendapati tindakan yang merugikan bagi perusahaan serta menyajikan rekomendasi kontrol dari kami.

2. Metode Penelitian

Dalam penelitian ini berfokus pada AP012 *Manage risk,* menganalisis risiko menggunakan COBIT 5 *for risk.* Dalam proses evaluasi manajemen risiko terdapat tiga tahapan dapat dijelaskan pada halaman selanjutnya.

2.1 Pengumpulan data

Melakukan studi *literatur*, tinjauan terhadap proses bisnis perusahaan, pengamatan kondisi perusahaan serta melakukan wawancara dan kuisoner, Untuk wawancara terhadap pemilik perusahaan agar mendapatkan informasi tentang kondisi terkait risiko yang pada perusahaan. Sedangkan untuk responden kuisoner adalah pengguna pihak internal perusahaan tanpa mengambil pihak eskternal perusahaan. Kuisoner berisi mengenai penentuan kriteria empat dampak berdasarkan COBIT 5 *for risk*. Selanjutnya risiko diidentifikasi berdasarkan hasil pemetaan.

2.2 Analisis data

Dalam tahap ini menganalisis data yang diperoleh pada tahap pengumpulan data berupa daftar risiko perusahaan. Analisis data membahas mengenai kategori risiko, tipe-tipe risiko serta skenario risiko berdasarkan COBIT 5 *for risk*. Skenario risiko dibagi dua, yaitu skenario positif dan negatif.

2.3 Analisis risiko

Setelah dilakukan analisis data selanjutnya melakukan penilaian risiko berdasarkan frekuensi dan dampak risiko perusahaan. Dalam melakukan penilaian risiko penentuan berapa kali kejadian risiko pernah terjadi pada perusahan dalam periode satu tahun serta dilakukan dengan menghitung rata-rata dampak risiko dan memunculkan tingkatan risiko. Selanjutnya kontrol yang tepat untuk setiap risiko sesuai proses pemetaan COBIT 5 dan empat tindakan respon terhadap risiko yang mungkin diterapkan, yaitu *avoid, mitigate, transfer, accept* berdasarkan COBIT 5 *for risk*. Tambahan dari kami akan membuatkan rekomendasi kontrol terhadap risiko yang ada, dikarenakan setiap risiko tidak semuanya *mitigate* ada juga risiko yang *transfer.*

3. Hasil dan Pembahasan

3.1 Pengumpulan data

Dari serangkaian studi *literatur*, pengamatan terhadap proses bisnis, pengamatan kondisi perusahaan, peneliti memperoleh daftar risiko membahas keterangan risiko dan penyebab risiko perusahaan. Tabel 1 menunjukkan hasil perolehan daftar risiko perusahaan.

Tabel 1. Daftar risiko

No	Risiko	Keterangan	Penyebab
1	Salah *input* data kiriman *customer*	Data kiriman tidak sesuai efek lambat *update* status pengiriman	Pengguna tidak teliti *entry* data pengiriman dikarenakan banyaknya kiriman atau tujuan kiriman tidak jelas

2	Layanan tidak bisa jalan	Tiba-tiba sistem tidak jalan maka layanan tidak berfungsi semuanya	*Software* erorr tidak bisa diakses karena *troubleshooting* membutuhkan waktu lama
3	Pencurian data pelanggan	Pencurian data pelanggan dilakukan staf perusahaan	Beberapa penyimpanan data pelanggan masih ada yang berupa *hardcopy*

3.2 Analisis data

Setelah dilakukannya identifikasi terhadap daftar risiko, selanjutnya tahap ini menentukan tipe risiko, kategori risiko dan skenario risiko. Dalam melakukan pemetaan kategori risiko berdasarkan kategori yang ditentukan dalam COBIT 5 untuk risiko terdapat dua puluh kategori risiko yang tersedia [3]. Kemudian dalam menentukan tipe risiko terdapat tiga jenis tipe, menurut [3] :

- Risiko pemberdayaan manfaat / nilai TI (tipe 1) — Terkait dengan peluang (yang terlewatkan) untuk menggunakan teknologi untuk meningkatkan efisiensi atau efektivitas proses bisnis atau sebagai pemacu untuk inisiatif bisnis baru.
- Program TI dan risiko pengiriman proyek (tipe 2) —Disosiasi dengan kontribusi TI untuk solusi bisnis yang baru atau lebih baik, biasanya dalam bentuk proyek dan program.
- Operasi TI dan risiko penyampaian layanan (tipe 3) — Terkait dengan stabilitas operasional, ketersediaan, perlindungan, dan pemulihan layanan TI, yang dapat membawa penghancuran atau pengurangan nilai bagi perusahaan.

'P' menunjukkan kecocokan primer (tingkat lebih tinggi) dan 'S' mewakili kecocokan sekunder (tingkat lebih rendah), sedangkan sel kosong menunjukkan bahwa kategori risiko tidak relevan untuk skenario risiko yang dihadapi.

Tabel 2. Tipe risiko

No	Kategori risiko	Risiko	Tipe Risiko		
			T1	T2	T3
1	*Staff operation (human error and malicious intent)*	Salah *input* data kiriman	S	S	P
2	*Software*	Layanan tidak jalan	S	S	P
3	*Information*	Pencurian data pelanggan	S	S	P

Setelah dilakukan penentuan tipe risiko setelah itu melakukan sebuah skenario risiko, skenario risiko dibagi menjadi dua jenis, yaitu skenario positif dan skenario negatif. Skenario positif menunjukkan risiko yang telah diidentifikasi tidak terjadi pada perusahaan sehingga menggambarkan proses bisnis perusahaan yang berjalan lancar. Sedangkan skenario negatif menunjukkan bahwa risiko perusahaan sedang terjadi, akibatnya menganggu perusahaan.

Tabel 3. Skenario risiko

No	Risiko	Skenario

		Skenario Positif	Skenario negatif
1	Salah input data kiriman	Pengguna mengisi data kiriman dengan benar dan sesuai sehingga akibatnya tidak lambat *update* status pengiriman	Pengguna dalam mengisi data kiriman tidak sesuai sehingga terjadi lambat *update* status pengiriman
2	Layanan tidak jalan	Pengguna dapat mengandalkan sistem ini dalam menjalankan proses bisnis dan permintaan layanan.	Pengguna tidak dapat menjelankan sistem layanan dikarenakan mengalami gangguan

3.3 Analisis risiko

Penentuan nilai risiko ditentukan pada frekuensi *value* berapa kali kejadian dalam setahun risiko perusahaan serta terjadinya dampak (*magnitude).* Untuk mengetahui rentang frekuensi yang digunakan dalam penentuan prioritas risiko telah disajikan pada Tabel 4.

Tabel 4. Skala frekuensi risiko

Frekuensi *value*	Frekuensi	Deskripsi
1	N = 0,1	*Very Low* Kemungkinan kecil, cenderung terjadi kurang dari 0,1 kali dalam setahun
2	0,1 < N = 1	*Low* Jarang, cenderung terjadi antara 0,1-1 kali dalam setahun.
3	1 < N = 10	Moderate Terkadang terjadi biasanya terjadi antara 1-10 kali dalam setahun
4	10 < N = 100	High Dapat terjadi, cenderung terjadi antara 10-100 kali dalam setahun.
5	100 < N	Very High Sering terjadi, biasanya terjadi lebih dari 100 kali setahun

Dampak risiko bedasarkan COBIT 5 *for risk* memiliki empat kriteria, seperti yang ditunjukkan pada Tabel 5. Untuk nilai produktivitas mengukur kerugian yang dikeluarkan selama periode satu tahun. Sedangkan biaya tanggapan menentukan biaya yang harus dikeluarkan oleh bymatrans untuk menangani kerugian yang terjadi setiap risiko yang terjadi. Selain itu terdapat nilai keunggulan kompetitif yang diukur dari kepuasan pengguna yang disebabkan oleh risiko setelah itu kriteria hukum mengukur jumlah denda yang harus dibayar perusahaan akibat risiko yang terjadi pada perusahaan sesuai dengan hukum. Nilai dampak risiko yang diperoleh membentuk nilai rata-rata dampak risiko diperoleh dari perhitungan jumlah nilai dampak dibagikan empat dampak kriteria

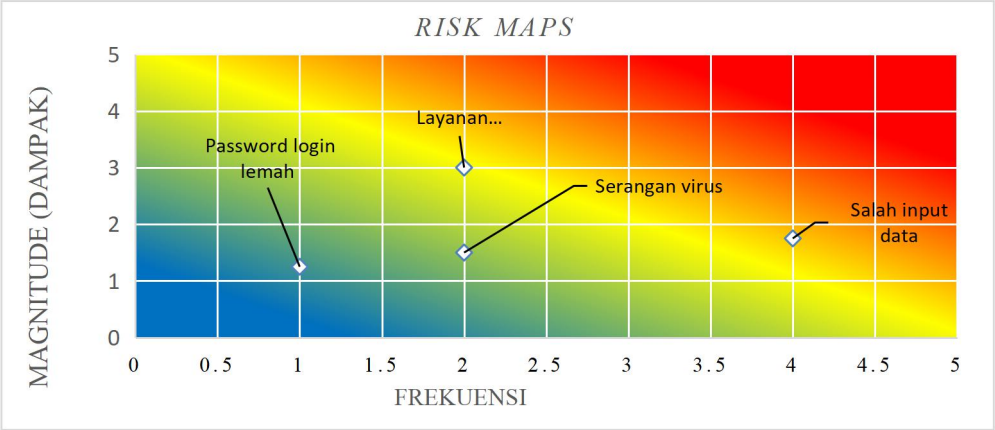
dan menghasilkan nilai rata-rata dampak risiko. Nilai frekuensi, nilai produktivitas, nilai biaya tanggapan, nilai keungguan kompetitif, nilai hukum diperoleh dari hasil kuisoner. Rincian hasil penilaian dampak risiko yang telah disajikan dapat diketahui pada Tabel 6. Dalam mengetahui tingkatan prioritas risiko diperlukan penggabungan antara nilai frekuensi dan nilai rata-rata dampat sehingga menghasilkan sebuah peta risiko *(risk maps*). Berikut penyajian *risk maps* dapat dilihat pada Gambar 1 *Risk maps.* Penjelasan terkait *risk maps* disajikan dalam bentuk tabel, Berikut rincian penjelasan dari *risk maps,* Dapat dilihat Tabel 7.

Tabel 5. Skala dampak risiko

Peringkat dampak	Dampak			
	Produktivitas	Biaya Tanggapan	Keunggulan kompetitif	Hukum
1	0,1%<I≤1%	100K<I≤Rp1juta	I ≤ 1	<Rp1 juta
2	1%<I≤3%	1juta<I≤Rp10juta	1 < I ≤ 1,5	<Rp10 juta
3	3%<I≤5%	10juta<I≤Rp100 juta	1,5 < I ≤ 2	<Rp100 juta
4	5%<I≤10%	100juta<I≤Rp500 juta	2 < I ≤ 2,5	<Rp500 juta
5	10%<I	Rp500 juta<I	2,5 < I	>Rp500 juta

Tabel 6. Nilai frekuensi dan dampak risiko

No	Risiko	Frekuensi	Produktivitas	Biaya tanggapan	Keunggulan kompetitif	Hukum	Rata-rata dampak
1	Salah input data kiriman	4	1	1	4	1	1,75
2	Layanan tidak jalan	2	4	3	4	1	3
3	Serangan virus	2	1	1	3	1	1,5
4	Login password lemah	1	1	1	2	1	1,25



Gambar 1. Risk maps

Tabel 7. Penjelasan risk maps

No	Risiko	Frekuensi	Rata-rata dampak	Tingkatan risiko
1	Salah input data kiriman	4	1,75	*High*
2	Layanan tidak jalan	2	3	*High*
3	Serangan virus	2	1,5	*Medium*
4	Login password lemah	1	1,25	*Low*

Setelah dilakukan penilaian risiko selanjutnya penentuan langkah mitigasi berdasrkan proses COBIT 5. Kemudian diambil beberapa aktivitasnya yang relevan dengan proses yang ditentukan dipilih untuk diterapkan pada perusahaan. Tabel 8 merangkum proses COBIT 5 yang sesuai dengan kategori risiko.

Tabel 8. Proses Cobit 5

No	Kategori risiko	Proses COBIT 5
1	*Staff operation*	DSS01 *Manage Operations*
3	*Malware*	DSS01 *Manage Operations*
4	*IT expertise and skill*	AP007 Manage Human Resource
5	*Infrastructure*	DSS05 *Manage Security Services*
6	*Logical Attack*	AP0013 *Manage Security*

Selanjutnya ialah menganalisis langkah-langkah mitigasi yang ditentukan berdasrkan tingkat prioritas risiko. Untuk risiko tingkat tinggi dan normal, langkah-langkah mitigasi akan dijelaskan secara terperinci sesuai aktivitas untuk meminimalkan kerugian perusahaan yang akan terjadi. Risiko tingkat tinggi dipetakan kedalam manajemen utama yang sesuai pada proses COBIT 5 *for risk* serta rekomendasi dari kami. Berikut perincian dari pemetaan COBI 5 pada Tabel 9

Tabel 9. Langkah mitigasi dan rekomendasi

No	Kategori risiko	Risiko	Tingkatan risiko	Respon risiko	Proses COBIT 5	Langkah mitigasi	Rekomendasi
1	*Staff operation (human error and malicious intent)*	Salah *input* data kiriman	*High*	*Mitigate*	DSS01.01 *Perform operational procedures*	Memilihara dan melakukan prosedur operasiona dengan handal Aktivitas : Diharapkan semua data yang telah diproses secara akurat, dan tepat waktu	Menyedikan aplikasi tanda terima pada bag.pengiriman

Tabel 9. Langkah mitigasi dan rekomendasi (lanjutan)

No	Kategori risiko	Risiko	Tingkatan risiko	Respon risiko	Proses COBIT 5	Langkah mitigasi	Rekomendasi
2	*Software*	Layanan tidak jalan	*High*	*Transfer*			1 .Dilakukan pengujian dan memperbarui layanan secara berkala 2 .Menerapkan DRP(*Disaster Recovery Plan*)

4. Kesimpulan

Dari hasil penelitian ini pada PT.BTM terkait risiko yang ada pada perusahaan, dengan menggunakan *framework* COBIT 5 *for risk* sebagian risiko yang tingakatan *high* berada dalam kategori risiko *Staff operation (human error and malicious intent)* dan *software.* Langkah-langkah mitigasi risiko dari kategori risiko *staff operation* dapat digunakan meminimalkan kesalahan staf. Pada DSS01 Memilihara dan melakukan prosedur operasional dan tugas operasional dengan handal proses ini melibatkan staf perusahaan agar semua data yang telah diproses secara akurat, dan tepat waktu kontrol yang diberikan berisi menyediakan aplikasi untuk bagian pengiriman agar memberikan *output* sesuai layanan perusahaan serta untuk risiko *software* tidak ada langkah mitigasi dikarenakan risikot tersebut dibagikan tetapi memiliki rekomendasi dari kami mengenai dilakukan pengujian dan meperbarui layanana secara berkala. Diharapkan hasil penelitian ini membantu pembuat keputusan perusahaan untuk dilakukan strategis.

Referensi :

[1] H. S. A. Ahmed, “COBIT 5 for Risk — A Powerful Tool for Risk Management,” pp. 1–5, 2017.
[2] NIST, “Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology,” p. 54, 2002.
[3] ISACA, “for Risk,” pp. 1–52, 2013.
[4] D. Tan, “Information Security Reading Room Quantitative Risk Analysis Step-By-Step,” 2019.
[5] H. M. Astuti, F. A. Muqtadiroh, E. W. Tyas Darmaningrat, and C. U. Putri, “Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk,” *Procedia Computer Science*, 01-Jan-2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917329599. [Accessed: 22-Mar-2019].
[6] D. R. Indah and M. A. Firdaus, “Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk,” *Proceeding 1st Int. Conf. Comput. Sci. Eng.*, pp. 113–118, 2014.
[7] S. Nasional, S. Informasi, T. A. Megawati, H. M. Astuti, and A. Herdiyanti, “PENGELOLAAN RISIKO ASET TEKNOLOGI INFORMASI PADA PERUSAHAAN PROPERTI PT XYZ , TANGERANG BERDASARKAN,” no. September, 2014.